Alternate proof of fact:

Let $V = |1\rangle\langle 1| \otimes U + |0\rangle\langle 0| \otimes \mathbb{1}$

$V^\dagger = |1\rangle\langle 1| \otimes U^\dagger + |0\rangle\langle 0| \otimes \mathbb{1}$

$$V^\dagger h V = \frac{|1\rangle\langle 1| \otimes \mathbb{1} - |1\rangle\langle 0| \otimes \mathbb{1} - |0\rangle\langle 1| \otimes \mathbb{1} + |0\rangle\langle 0| \otimes \mathbb{1}}{2}$$

$$= |-\rangle\langle -| \otimes \mathbb{1}.$$

So groundstates of $V^\dagger h V$ are states of the form

$|+\rangle \otimes |\psi_0\rangle.$

and $V^\dagger h V$ is a projector. So groundstates of h

are states of the form $V|+\rangle \otimes |\psi_0\rangle$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle|\psi_0\rangle + |1\rangle U|\psi_0\rangle\right).$$

Apply this intuition to general Hamiltonian circuit

$$h_t = \frac{1}{2}\left(|t\rangle\langle t| \otimes \mathbb{1} - |t\rangle\langle t-1| \otimes g_t - |t-1\rangle\langle t| \otimes g_t^\dagger + |t-1\rangle\langle t-1| \otimes \mathbb{1}\right)$$

Each term h_t acts on time register + 2 extra qubits def. by g_t.

Same calculation will tell us that for $|\psi\rangle = \sum_t |t\rangle|\psi_t\rangle$

that

$$\langle\psi|h_t|\psi\rangle = \Big\| \, |\psi_t\rangle - g_t|\psi_{t-1}\rangle \Big\|^2 .$$

But how do all the pieces act together? Analyze a rotation.

$$V = \sum_{t=0}^{T} |t\rangle\langle t| \otimes g_t \cdots g_1$$

$$V^\dagger = \sum_{t=0}^{T} |t\rangle\langle t| \otimes g_1^\dagger \cdots g_t^\dagger .$$

$$V^\dagger h_t V = \frac{1}{2}\Big(|t\rangle\langle t| \otimes \mathbb{1} - |t-1\rangle\langle t| \otimes \mathbb{1} - |t\rangle\langle t-1| \otimes \mathbb{1} + |t-1\rangle\langle t-1| \otimes \mathbb{1} \Big)$$

$$= \frac{1}{\sqrt{2}}\Big(|t\rangle - |t-1\rangle\Big)\frac{1}{\sqrt{2}}\Big(\langle t| - \langle t-1|\Big) \otimes \mathbb{1} .$$

So, $V^\dagger\left(\sum_{t=1}^{T} h_t\right)V =$

$$\frac{1}{2}\begin{pmatrix} 1 & -1 & & & \\ -1 & 2 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & -1 & 2 & -1 \\ & & & -1 & 1 \end{pmatrix} \otimes \mathbb{1} .$$

This is a special matrix. It is the Laplacian of a line graph and also a circulant matrix. (also tri-diagonal)

$\lambda_0 = 0$, eigenvector $|\Psi_0\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes |\psi_0\rangle$ ← for any $|\psi_0\rangle$

$\lambda_1 \geq \frac{c}{T^2}$ ← exercise / intuition from graph mixing time.

So, removing rotation by V:

$$H_{prop} = \sum_{t=0}^{T} h_t$$ is a Hamiltonian with

ground-energy $= 0$, groundstates of the form $\underbrace{\frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes g_t \cdots g_1 |\psi_0\rangle}_{\text{known as a history state}}$

for any state $|\psi_0\rangle$

highly degenerate groundspace.

and first non-zero energy of $\geq c/T^2$.

Therefore, $H_{prop} \geq \frac{c}{T^2}\left(\mathbb{1} - \Pi_{prop}\right)$ ← projector onto span of history states

Next: Adding checks for ancilla and output and computing overall eigenvalues to make sure cheating provers are detected.

History states just check evolution of the computation

To check output of computation, we want a term that checks that when the time register is set to T, the first qubit is in the $|1\rangle$ state.

$$H_{out} = |T\rangle\langle T|_{time} \otimes |0\rangle\langle 0|_1$$

Penalizes being time T and first qubit = 0.

To check input, we need to make sure that all the ancilla registers of the computation were set to $|0\rangle$.

$$H_{in} = \sum_{j=1}^{m} |0\rangle\langle 0|_{time} \otimes |1\rangle\langle 1|_{ancilla(j)}$$

$H_{out} + H_{in}$ is a commuting Hamiltonian meaning every pair of local terms commute.

Each local term is a projector. So $H_{out} + H_{in}$ has an integer spectrum.

$$H_{out} + H_{in} \geq \left(\mathbb{1} - \Pi_{inout}\right)$$

projector onto passing all in & out checks.

<u>Claim</u> $H = H_{prop} + H_{out} + H_{in}$ suffices as a Ham.

Intuition: Let $|\psi\rangle = \sum_{t=0}^{T} |t\rangle|\varphi_t\rangle$ ← unnormalized.

so $\| |\psi\rangle \| = 1 \Rightarrow \sum_{t=0}^{T} \| |\varphi_t\rangle \|^2$

h_t gives energy $\quad \| |\varphi_t\rangle - g_t |\varphi_{t-1}\rangle \|^2$

H_{in} gives energy $\sum_{j=1}^{m} \| \langle 1|_{ancilla(j)} |\varphi_0\rangle \|^2$

H_{out} gives energy $\| \langle 0|_1 |\varphi_T\rangle \|^2$

Recall $$V = \sum_{t=0}^{T} |t\rangle\langle t| \otimes g_t \cdots g_1 .$$

Let $$|\mu\rangle = V^{\dagger}|\psi\rangle = \sum_t |t\rangle|\mu_t\rangle$$

where $$|\mu_t\rangle = g_1^{\dagger} \cdots g_t^{\dagger} |\psi_t\rangle.$$

Then

h_t gives energy $$\| |\mu_t\rangle - |\mu_{t-1}\rangle \|^2$$

H_{in} gives energy $$\sum_{j=1}^{m} \| \langle 1|_{ancilla(j)} |\mu_0\rangle \|^2$$

H_{out} gives energy $$\| \langle 0|_1 C |\mu_T\rangle \|^2$$

If satisfiable then $\exists$ good choice $|\mu\rangle$ for all $|\mu_0\rangle \ldots |\mu_t\rangle$.

When unsatisfiable, in order for H_{in} and H_{out}

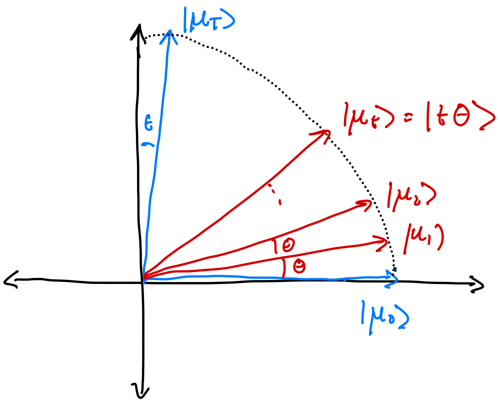
energy to be small... $|\mu_0\rangle$ and $|\mu_T\rangle$ are orthogonal.

For intuition only: The following is not the lowest energy state.

Cartoon: $|\mu_0\rangle = |0\rangle$ and $|\mu_1\rangle \approx |1\rangle$ in some 2D space

(can be formal due to Jordan's lemma)

Then ideal $|\mu_t\rangle$ would be $|t\theta\rangle$ for $\theta = \frac{\pi}{2T}$ to minimize H_{prop} energy.



Then $\langle\psi|H|\psi\rangle$

$$= \langle\mu|V^{+}HV|\mu\rangle$$

$$\leq \langle\mu|V^{+}h_t V|\mu\rangle$$

$$= T \cdot \sin^2\theta$$

$$= O\left(\frac{1}{T}\right).$$

We will prove a lower bound of $\Omega\left(\frac{1}{T^3}\right)$ in the next class.

Pf. Consider a (yes) instance of QCIRCUIT SAT.

i.e. $\exists\ |\psi\rangle$ s.t. $C(|\psi\rangle)$ accepts w pr $\geq 1-\epsilon$.

Then let $|\Psi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes g_t \cdots g_1 |\psi, 0^m\rangle$

the History state of $|\psi\rangle$. By construction,

$\langle\Psi| H_{prop} |\Psi\rangle = 0$

$\langle\Psi| H_{in} |\Psi\rangle = 0 \qquad \Rightarrow \qquad \langle\Psi|H|\Psi\rangle \leq \epsilon.$

$\langle\Psi| H_{out} |\Psi\rangle \leq \epsilon$

What about a (no) instance of QCircuit SAT?

Recall the max success prob. of a QCircuitSAT instance was $\cos^2\Theta$ where Θ was the angle between $\mathbb{1}_{2^n} \otimes |0\rangle\langle 0|^m$ and $C^\dagger(|1\rangle\langle 1| \otimes \mathbb{1}_{2^{n+m-1}})C$ projectors.

If max success prob is small ($\leq \epsilon$) then Θ is large (near $\frac{\pi}{2}$).

as $\cos^2\Theta = \epsilon$.

We want to show that $\lambda_{min}(H)$ is not super small.

Since $H_{prop} \geq \frac{c}{T^2}(\mathbb{1} - \Pi_{prop})$

it suffices to show lower bound on:

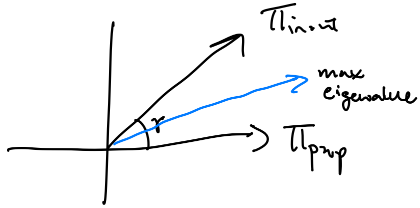
$$\lambda_{min}\left(\frac{c}{T^2}(\mathbb{1} - \Pi_{prop}) + (\mathbb{1} - \Pi_{inout})\right)$$

$$\geq \frac{c}{T^2}\lambda_{min}\left((\mathbb{1} - \Pi_{prop}) + (\mathbb{1} - \Pi_{inout})\right)$$

$$\geq \frac{c}{T^2}\left(2 - \lambda_{max}\left(\Pi_{prop} + \Pi_{inout}\right)\right)$$

$$= \frac{c}{T^2}\left(2 - 2\cos^2\frac{\gamma}{2}\right) = \frac{2c}{T^2}\sin^2\frac{\gamma}{2}.$$

where γ = angle between Π_{prop} and Π_{inout}



To do this, let's bring back

$$V = \sum_{t=0}^{\tau} |t\rangle\langle t| \otimes g_t \cdots g_1.$$

We know that

$$V^\dagger \Pi_{prop} V = \text{projector onto states} \left\{ |h_\psi\rangle := \frac{1}{\sqrt{T+1}} \sum_{t=0}^{\tau} |t\rangle \otimes |\psi\rangle \right\}$$

$$V^\dagger \Pi_{in+out} V = \left(|T\rangle\langle T| \otimes C^\dagger (|1\rangle\langle 1|_1 \otimes \mathbb{1}) C \right) \cdot$$

$$\left(|0\rangle\langle 0| \otimes \mathbb{1}_{2^m} \otimes |0^m\rangle\langle 0^m| \right)$$

terms commute.

$$\gamma = \text{angle}\left(\Pi_{prop}, \Pi_{in+out} \right) = \text{angle}\left(V^\dagger \Pi_{prop} V, V^\dagger \Pi_{in+out} V \right)$$

To calculate angle between spaces :

$$\cos^2 \gamma = \max_{|\psi\rangle} \langle h_\psi | \Pi_{in+out} | h_\psi \rangle$$

$$= \max_{|\psi\rangle} \frac{1}{T+1} \sum_{t=0}^{1} \langle t| \langle \psi | \Pi_{in+out} |t\rangle |\psi\rangle$$

$$= \max_{|\psi\rangle} \frac{T-1}{T+1} + \frac{1}{T+1} \left(\langle \psi | C^\dagger (|1\rangle\langle 1| \otimes \mathbb{1}) C |\psi\rangle + \langle \psi | \mathbb{1}_{2^m} \otimes |0^m\rangle\langle 0^m| \, |\psi\rangle \right)$$

$$= \frac{T-1}{T+1} + \frac{1}{T+1} \, 2 \cos^2 \frac{\theta}{2}$$

as optimal $|\psi\rangle$ is midway between projectors $C^\dagger(|1\rangle\langle 1|_1 \otimes \mathbb{1})C$

and $\mathbb{1}_{2^m} \otimes |0^m\rangle\langle 0^m|$ which are θ apart.

Recall $\sqrt{\epsilon} = \cos\theta = 2\cos^2\frac{\theta}{2} - 1 \Rightarrow$

$\Rightarrow 2\cos^2\frac{\theta}{2} = 1-\sqrt{\epsilon} \Rightarrow$

$$\cos^2\gamma = \frac{T-1}{T+1} + \frac{1}{T+1}\left(1+\sqrt{\epsilon}\right) = 1 - \frac{(1-\sqrt{\epsilon})}{T+1}.$$

$$\sin^2\frac{\gamma}{2} = \frac{1-\cos^2\gamma}{2} = \frac{1-\sqrt{\epsilon}}{2(T+1)}.$$

Therefore, $\lambda_{min}(H) \geq \frac{2c}{T^2}\left(\frac{1-\sqrt{\epsilon}}{T+1}\right) = \Omega\left(\frac{1}{T^3}\right)$

for small ϵ.

So if yes instance, $\lambda_{min}(H) \leq \epsilon$

if no instance, $\lambda_{min}(H) \geq \frac{1}{T^3}$.

To complete pf of QMA-hardness, first use amplification to convert any QCIRCUITSAT problem to $(1-\epsilon, \epsilon)$ amplification for $\epsilon < \frac{1}{T^3}$. Then apply the circuit-to-Hamiltonian construction.

A more sophisticated analysis proves that no instances map to $\Omega\left(\frac{1}{T^2}\right)$.

Note that we only proved QMA-hardness for $O(\log T) = O(\log n)$ local Hamiltonians. Your homework includes a transform to 5-local Hamiltonians.

This will yield a Hamiltonian acting on $T+n+m$ qubits.

Also, we only proved it was QMA-hard to estimate $\lambda_{min}(H)$ to $\frac{1}{T^3} \sim \frac{1}{N^3}$ where N is the number of qubits in the Ham.

It may be easier to get a coarser approximation

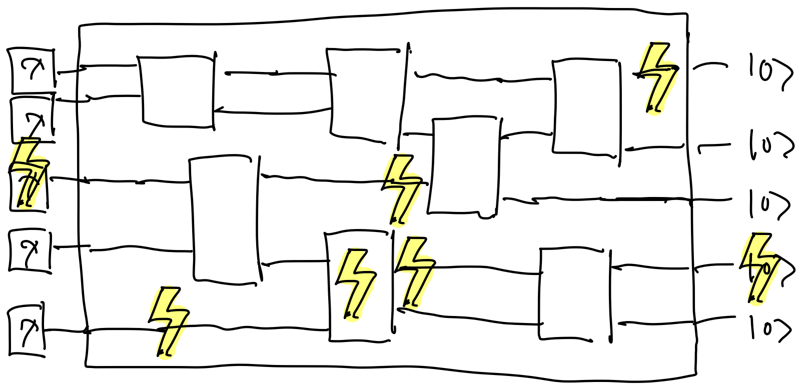
Quantum Error Correction.

Until knew, we have talked about perfect application of gates and perfect initialisations of q. states.

What if that is not the case?

Error-correction gives a theory of how to recover information in the presence of noise.

Biggest block to our construction of large scale q. computers.
Quantum computation is more succeptible to noise than classical computation.



Errors can occur in <u>any</u> component...

How do we correct.

① A theory of correction for static q. information.

No computation occuring, just errors.

Run a sequence of corrections to return information back to original.

Quantum analog of reliable data storage.

Classical: CDs, SSDs, Harddrives, Pen and Paper

② Correction interspersed with computation

Called Fault-Tolerance and will be covered in Lecture 20 by guest lecturer Michael Beverland.

How do we correct classical information?

Theory: Rich. Practice: Redundancy.

WiFi/3G/4G : LDPC codes

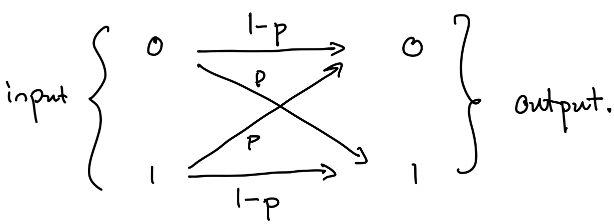
CD-Rom: Reed-Solomon codes

Computation: Run it thrice and take majority vote.

Reasonable because a classical bit in a modern transistor incurs an error with $pr < 10^{-15}$.

To analyze error-correction (theoretically), we first need a model for error.

Simplest model bit flip channel.



$$\rho \longmapsto \mathcal{E}(\rho) = p \cdot X \rho X + (1-p)\,\rho.$$

Notion holds for quantum also.

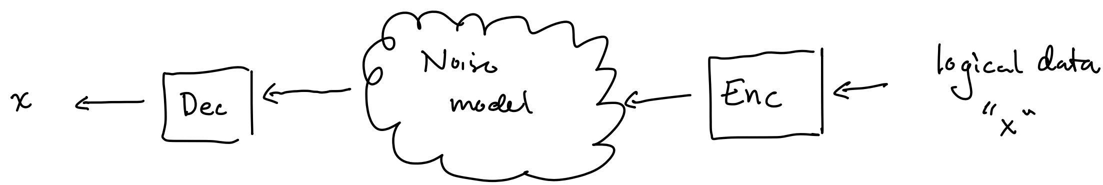
High level: A channel is a map from density matrices to density matrices consistent with q. mechanics axioms.

Bit flip on each bit:

$$\mathcal{L}(\mathbb{C}^{2^n}) \ni \rho \longmapsto \mathcal{E}^{\otimes n}(\rho).$$

$$\Pr[\text{no bit gets flipped}] = (1-p)^n \longrightarrow 0 \quad \text{as } n \longrightarrow \infty.$$

General procedure.



Easiest classical example: Repetition code.

$$\bar{0} := \mathrm{Enc}(0) = 0\cdots\cdots 0$$

$$\bar{1} := \mathrm{Enc}(1) = \underbrace{1\cdots\cdots 1}_{n \text{ times}}.$$

Assume $p < \frac{1}{2}$.

$$\mathrm{Dec}(y) = \begin{cases} 0 & \text{if } |y| < \frac{n}{2} \\ 1 & \text{if } |y| > \frac{n}{2} \end{cases}.$$

$$\Pr_{\text{error}}\left[\text{decoding is wrong}\right] = \Pr_{\text{error}}\left[\geq \tfrac{n}{2} \text{ bits flipped}\right] \leq e^{-\Omega(n)}$$

The 3 troubles of quantum error correction.

① Infinite collection of possible errors even just on one qubit.

② No-cloning theorem.

There is no unitary mapping $|0\rangle \mapsto |0\rangle|0\rangle$ and $|+\rangle \mapsto |+\rangle|+\rangle$

Therefore quantum repetition code doesn't make sense.

③ Measurements destroy quantum info.

How do we correct when measurement is perturbative?

Today: Shor's 9 qubit code + theory of EC.

Let's correct first for a specific subset of errors:

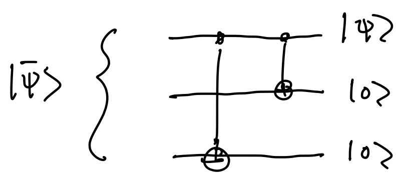
Single qubit X (bit flip), Z (phase flip), and XZ (bit + phase)

To correct just bit flip errors, appeal to classical intuition.

map $|0\rangle \mapsto |000\rangle$
$|1\rangle \mapsto |111\rangle$

Does not violate no cloning as we copy in 1 basis

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longmapsto |\bar{\psi}\rangle = \mathrm{Enc}|\psi\rangle = \alpha|000\rangle + \beta|111\rangle.$$

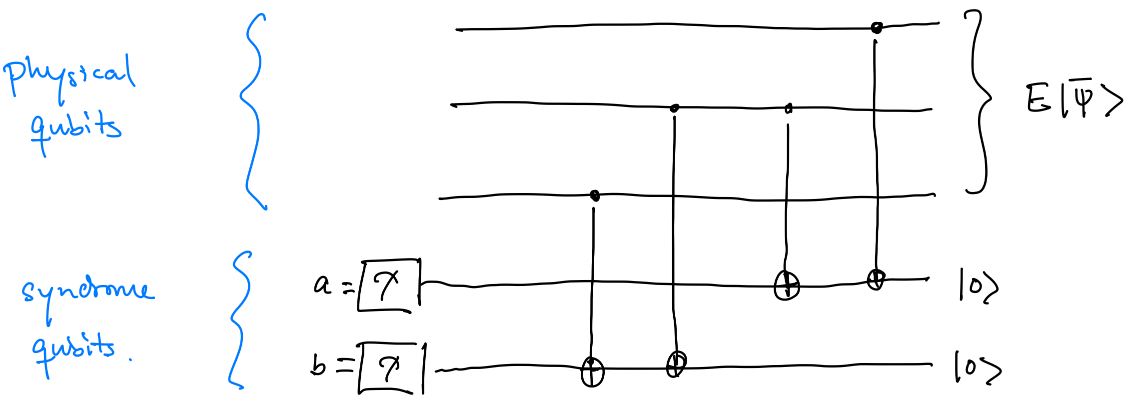


Say error occurs on middle qubit.

$$E|\bar{\psi}\rangle = \alpha|010\rangle + \beta|101\rangle.$$

Measuring would destroy superposition.

Instead, we compute error-syndromes and measure these.



If run on $|x,y,z\rangle$, then $a = x \oplus y$, $b = y \oplus z$.

$$a \oplus b = x \oplus z.$$

By linearity, when run on $E|\overline{\Psi}\rangle = \alpha|010\rangle + \beta|101\rangle$

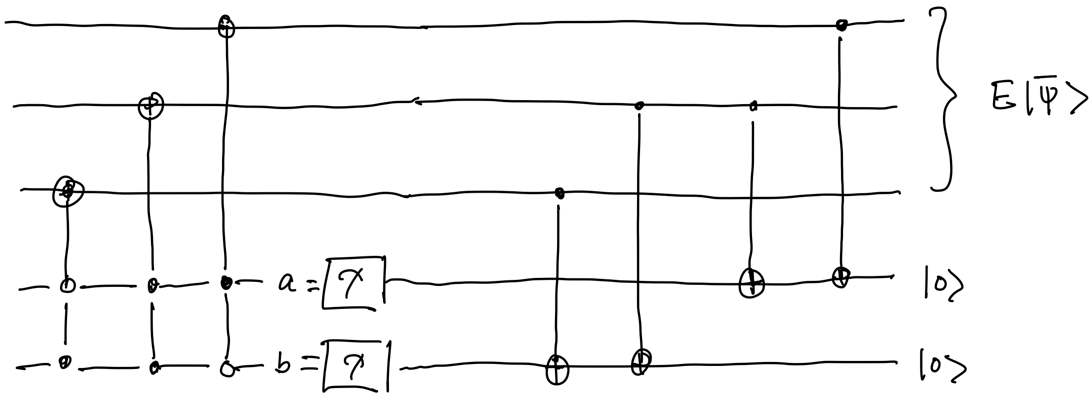
we get

$$\alpha|010\rangle|11\rangle + \beta|101\rangle|11\rangle$$

$$= \left(E|\overline{\Psi}\rangle\right) \otimes \underbrace{|11\rangle}_{\text{syndrome}}.$$

What happens for other bit flip errors?

Error	a	b
no error	0	0
1st qubit	1	0
2nd qubit	1	1
3rd qubit	0	1



After correction, we can discard the syndrome qubits (they are now unentangled by measurement).

$$\boxed{\text{Dec} = \text{Enc}^{-1} \circ \text{Correction}}.$$

Correcting only phase errors:

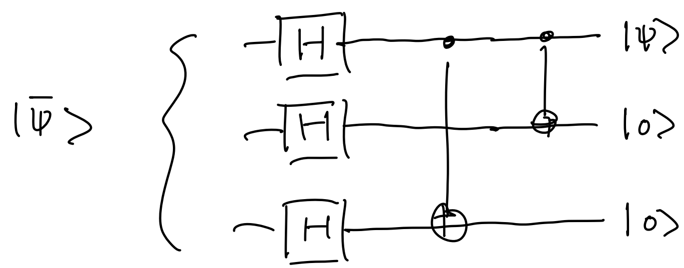
Note $HZH = X$. Phase errors are

bit flip errors in a different basis.

$|0\rangle \mapsto |+++\rangle$

$|1\rangle \mapsto |---\rangle$.

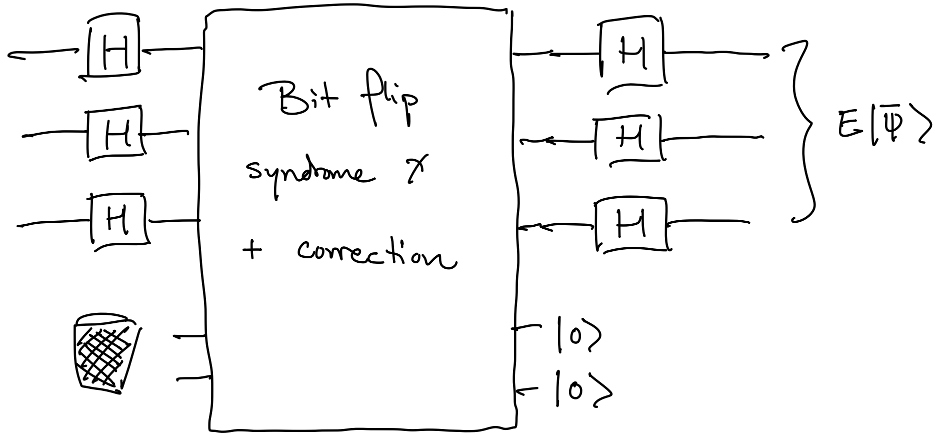
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \mapsto |\overline{\psi}\rangle = \alpha|+++\rangle + \beta|---\rangle.$$



Z error on 3rd qubit. Then

$$\alpha|+++\rangle + \beta|---\rangle \xmapsto{Z_3} \underbrace{\alpha|++-\rangle + \beta|--+\rangle}_{= H^{\otimes 3}\alpha|001\rangle + \beta|110\rangle}.$$

So correction circuit is easy to concoct.



Note if we encode in phase flip code but X_1 occurs then

$$\alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle \xmapsto{X_1} \alpha|{+}{+}{+}\rangle - \beta|{-}{-}{-}\rangle$$

New state will have syndrome $(0,0)$ for phase flip code and corresponds to applying Z on underlying logical information.

Same with phase flip for bit flip encoding.

How do we combine to get both error corrections?

Ans: Encode in one code and then in the other.

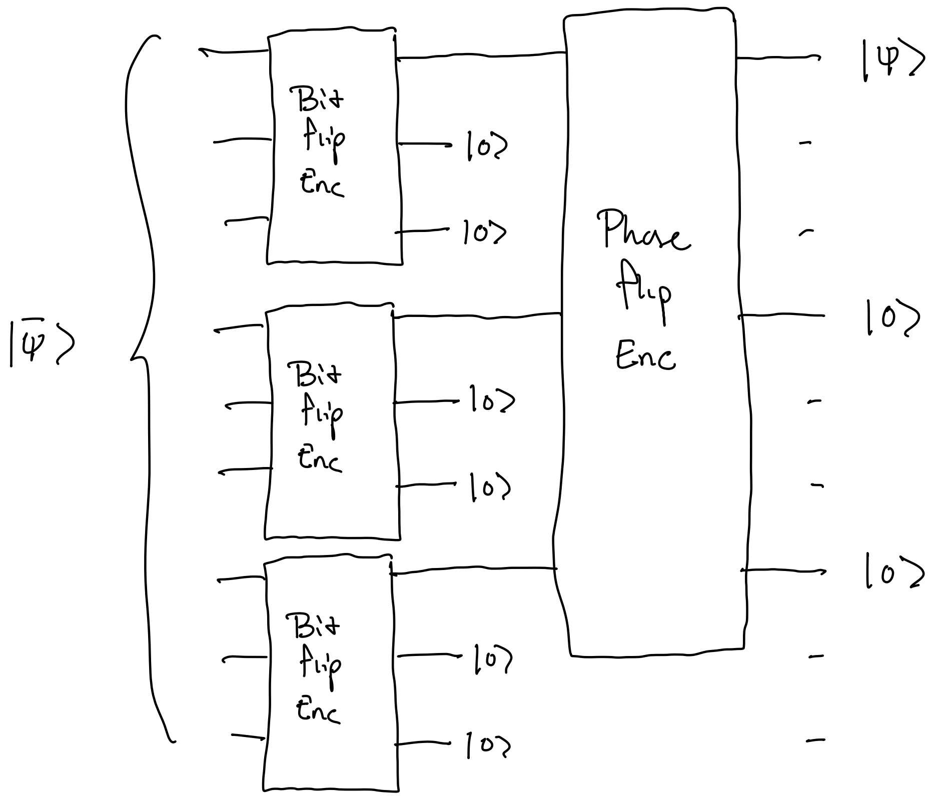
$$|0\rangle \longmapsto |+\rangle^{\otimes 3} \longmapsto \frac{1}{\sqrt{8}}\left(|000\rangle + |111\rangle\right)^{\otimes 3}$$

$$|1\rangle \longmapsto |-\rangle^{\otimes 3} \longmapsto \frac{1}{\sqrt{8}}\left(|000\rangle - |111\rangle\right)^{\otimes 3}$$

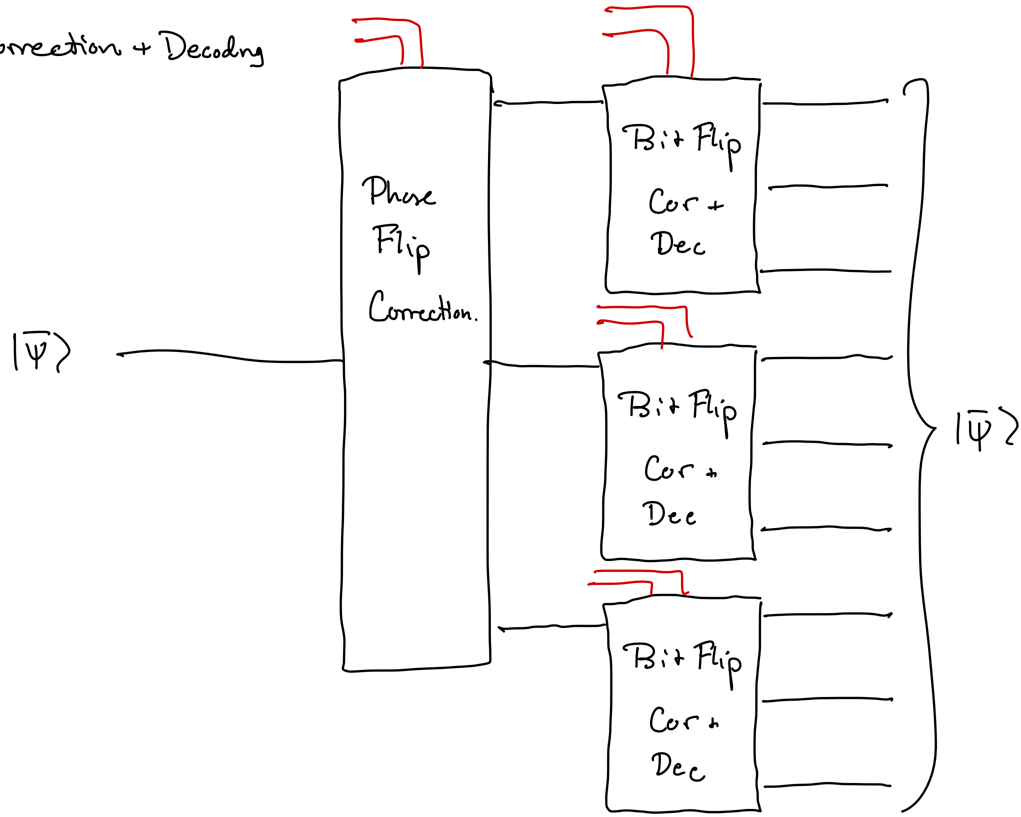
Could have also done in the other order

↑ But has different correction operators.

Encoding:



Correction + Decoding



This corrects any 1 bit flip error per triple and 1 phase flip error. To correct bit + phase flip error in the same qubit, both syndromes check.

<u>Fact</u>: Every Hermitian $H \in \mathbb{C}^{2\times 2}$ equals

$$H = \alpha \mathbb{1} + \beta X + \gamma (XZ) + \delta Z.$$

Next lectures:

1. What about infinite family of errors?

   (Rough answer: Pauli errors form a basis for all errors)

2. Can we correct without decoding? (Yes)

3. How do we encode more than 1 qubit of logical information?

Is there a general theory of why this is working?

A general theory of q. error correction.

(Slides as there are a lot of drawings)

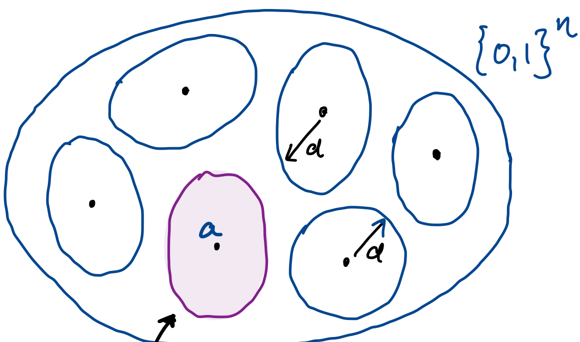
Part 2 (of Lec 17)

An (abridged) theory of classical error correction.

A subset $C \subseteq \{0,1\}^n$ is a code encoding k bits into n bits if $|C| = 2^k$.

The distance of the code is $d = \min_{\substack{x, y \in C \\ x \neq y}} d_H(x, y)$

the min number of bits required required to flip some $x \in C$ to $y \in C$. A code of distance d can correct $\lfloor \frac{d-1}{2} \rfloor$ errors.



all words that correct to a

Typically, when people talk about classical error correction they are talking about linear codes.

$k = \dim C$ and $C = \ker A \leftarrow$ check matrix.

Notation: $C = [n, k, d]$ code with locality ℓ if $C = \ker A$ with A being ℓ-row & -column sparse.

<u>Ex</u>. $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

$Ax = 0$

equals

$x_1 \oplus x_2 = x_2 \oplus x_3 = 0$.

$C = [3, 1, 3]$ code.

$$d = \min_{\substack{x \neq y \\ x, y \in C}} d_H(x, y) = \min_{\substack{x \in C \\ x \neq 0}} |x|.$$